DETAILED ACTION

1. Claims 1-8 have been presented for examination.

Priority

2. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d).

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 5-8 are rejected under 35 U.S.C. 101 as not falling within one of the four statutory categories of invention. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C. 101 must (1) be tied to particular machine, or (2) transform underlying subject matter (such as an article or material) to a different state or thing. *In Re Bilski*, 545 F.3d 943, 954 (Fed. Cir. 2008). The instant claims are neither positively tied to a particular machine that accomplishes the claimed method steps nor transform underlying subject matter, and therefore do not qualify as a statutory process. The method steps are broad enough that the claim could be completely performed mentally, verbally or without a machine nor is any transformation apparent.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for

> patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

6. Claims 2 and 6 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent Application Publication No. 2004/0120519 A1 to Joye et al., hereinafter Joye

7. As per claims 2 and 6, Joye teaches a secure communication system and method comprising:

a communications network (paragraph 0002, i.e. communication by means of a non-secure channel);

at a sending location on said network an encryptor (1) for providing a plurality of asymmetric encryptions of a message (M), each said encryption corresponding to a respective receiving location (1 to n) on said network (paragraphs 0015, 0016, i.e. encrypting message M), said encryptor comprising:

means (53 or 93) for deriving from said message (M) a first random number (r) (paragraphs 0016, 0025, i.e. random number u, random number r); and

means (57-0 to 57-n and 59-1 to 59-n, or 97-1 to 97-n and 99-1 to 99-(n-1) and 101-(-1) to 101-(n-1) and 103 and 105 and 107) for utilising the first keys (pk1 to pkn, or id1 to idn) of asymmetric encryption key pairs (pk1 to pkn and sk1 to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) together with said first random number (r) and said message (M) to generate said plurality of asymmetric encryptions of the message (paragraphs 0016, 0029, encrypting using the random number u and the recipient's public key); and, at each said receiving location (1 to n) on said network a decryptor (5) for decrypting the encryption of said plurality of encryptions which corresponds to that receiving location (1 to n) to provide said message (M), said decryptor (5) comprising means (71, 73, 75, or 111, 113, 115 or 131, 133, 135, 137, 139, 141) for utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption corresponding to the receiving location to recover the message (M) (paragraphs 0022, 0037-0038, i.e. decrypting the message M to recover random numbers u and r).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1 and 5 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,912,655 B1 to Zucker, hereinafter Zucker, in view of U.S. Patent No. 7,234,059 B1 to Beaver et al., hereinafter Beaver.

10. As per claims 1 and 5, Zucker teaches secure communication system and method comprising:

a communications network (column 1, lines 24-47, i.e. transmitting information from party A to party B);

at a sending location (i.e. party A) on said network:

(i) an encapsulator (1) for providing (a) a session key (K), and (b) a plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) . . . Ei(K) . . . En(K)), each said encryption corresponding to a respective receiving location (1 to n) on said network (column 1, lines 24-41, i.e. party A encrypts the random common symmetric key K using party B, C, and D's public keys for transmission to B, C, and D respectively); and

(ii) a symmetric encryptor (3) for utilising said session key (K) to encrypt a message (M) (column 1, lines 41-47, i.e. Party A encrypts message using random common symmetric key K); and,

at each said receiving location (1 to n) (parties B, C, D) on said network:

(i) a decapsulator (5) for decrypting the encryption of said plurality of encryptions (E1(K), E2(K), E3(K) . . . Ei(K) . . . En(K)) which corresponds to that receiving location (1 to n) to provide said session key (K) (column 1, lines 43-47, i.e. parties B, C, and D use their respective private keys to decrypt the encrypted common symmetric key K); and

(ii) a symmetric decryptor (7) for utilising the session key (K) to decrypt the message (M) (column 1, lines 43-47, i.e. using the decrypted common symmetric key K to decrypt the broadcast message),

said encapsulator (1) comprising:

means for utilising the first keys of asymmetric encryption key pairs (pk1 to pkn and ski to skn, or id1 to idn and S1 to Sn) of the intended recipients at the receiving locations (1 to n) to generate said plurality of asymmetric encryptions of the session key (E1(K), E2(K), E3(K) . . . Ei(K) . . . En(K)) (column 1, lines 24-41, i.e. party A encrypts the random common symmetric key K using party B, C, and D's public keys for transmission to B, C, and D respectively), said decapsulator (5) at each receiving location (1 to n) comprising:

means for utilising the second key (ski or Si) of the asymmetric encryption key pair (pki and ski, or idi and Si) of the recipient at the receiving location together with the asymmetric encryption (Ei(K)) corresponding to the receiving location to recover said symmetric key (column 1, lines 43-47, i.e. parties B, C, and D use their respective private keys to decrypt the encrypted common symmetric key K).

11. Zucker does not teach that the encapsulator comprises: a pseudo random number generator; symmetric key derivation means for deriving said session key from a first random number generated by said pseudo random number generator; means for utilising said first random number to generate a second random number; and using first and second random number to encrypt the session key; and

a decapsulator that recovers a random number from the encrypted data and generates a symmetric key from said first random number.

12. Beaver discloses generating a plurality of random numbers (Abstract) and wherein the symmetric key is generated from a token and the plurality of random numbers (Abstract, column 4, lines 13-64) and using the random number at the recipient to recover the symmetric key (column 4, lines 42-64).

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a pseudo random generator that generates a random number which in turn is used to generate another random number and using those two random number to encrypt the session key, while the receive uses the random number to recover a symmetric key, since Beaver

states at column 4, line 65 to column 5, line 3 that it provides a way for members of a group to perform authenticated communications while ensuring a message has not been altered.

Allowable Subject Matter

14. Claims 3, 4, 7, and 8 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

16. The following patents are cited to further show the state of the art with respect to encryption techniques, such as:

United States Patent Application Publication No. 2005/0198170 A1 to LeMay et al., which is cited to show a KEM-DEM patent application.

United States Patent No. 7,263,619 B1 to Kim, which is cited to show encrypting a message with a symmetric key and encrypting the symmetric key.

United States Patent No. 6,151,676 to Cuccia et al., which is cited to show data encrypted with a symmetric key and subsequently encrypting the symmetric key.

United States Patent No. 6,807,277 B1 to Doonan et al., which is cited to show encrypting a message and then encrypting the key used to encrypt said message.

United States Patent No. 6,675,296 B1 to Boeyen et al., which is cited to show sending e-mails encrypted with a random symmetric key and using the recipient's public key to encrypt the random symmetric key.

United States Patent No. 7,257,706 B1 to Zucker, which is cited to show a patent related to one that was used to reject the claims of the instant application.

United States Patent No. 7,260,724 B1 to Dickinson et al., which is cited to show a traditional PKI technology where a message is encrypted using a symmetric key and symmetric key is subsequently encrypted with the public key of the receiver.

United States Patent No. 6,574,733 B1 to Langford, which is cited to show a PKI system that uses a random number generator as a symmetric key generator.

United States Patent No. 6,567,914 B1 to Just et al., which is cited to show generating a symmetric key using a random number generator.

United States Patent No. 7,480,384 B2 to Peyravian et al., which is cited to show a PKI system using Diffie-Hellman and plural random numbers.

United States Patent Application Publication No. 2003/0037241 A1 to Campagna, which is cited to show a PKI that generates two random initialization vectors.

United States Patent No. 6,760,752 B1 to Liu et al., which is cited to show generating a random number, encrypting the message using the random number as a session key in a symmetric key encryption algorithm and encrypting the session key using a public key encryption algorithm and the recipient's public key.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian LaForgia whose telephone number is (571)272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edan Orgad can be reached on (571) 272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2439

clf